IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellant :	STONE et al.
Title:	SECURE TRACKING SYSTEM AND METHOD FOR VIDEO PROGRAM CONTENT
Appl. No.:	10/600,081
Filing Date:	6/20/2003
Examiner:	Jeremy S Duffield
Art Unit:	2427
Confirmation Number:	6842

REPLY BRIEF UNDER 37 C.F.R. § 41.41

Mail Stop Appeal Brief - Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This reply brief is filed pursuant to 37 C.F.R. § 41.41 in response to the Examiner's Answer dated September 1, 2010. No fee is believed to be due. However, if any fees are required, authorization is hereby given to charge any deficiency (or credit any balance) to the undersigned deposit account 19-0741.

TABLE OF CONTENTS

REAL PARTY IN INTEREST

The real party of interest is Verance Corporation, the assignee of the present application. This Application names Chris L. Stone and Scott Garen as inventors. The inventors each executed an assignment of the Application to Verance Corporation, having a place of business at 4435 Eastgate Mall Suite 350, San Diego, CA 92121. The assignment was recorded by the United States Patent and Trademark Office at Reel/Frame No. 016538/0469 on July 15, 2005.

RELATED APPEALS AND INTERFERENCES

Appellant is not aware of any related cases that will directly affect, be directly affected by, or have a bearing on the present appeal.

STATUS OF CLAIMS

Claims 2-4, 6, 7, 10-33, 35, 36, 38-40 and 42 have been finally rejected and are the subject of this appeal.

STATUS OF AMENDMENTS

No amendment was filed after the September 2, 2009, mailing date of the Final Office Action.

SUMMARY OF CLAIMED SUBJECT MATTER

Embodiments of the present invention relate to a system for tracking broadcast programs. The disclosed embodiments enable the identification of the original program at the point of origin and after it has been distributed through various distribution channels, such as broadcast, cable, Internet, and other transmission channels (page 1, lines 6-10). The reporting of the time and date of distribution/reception of the programs, as well as reporting possible alterations to the programs to the interested parties enables appropriate royalty payments to be collected and/or distributed (Id.).

One method of identifying the broadcast programs involves the use of watermarking techniques. Watermarking refers to embedding a unique identification code within the broadcast program such that it can be subsequently extracted in order to identify the program at various points of distribution (page 3, lines 3-7). Another identification technique is fingerprinting, which involves analyzing the inherent characteristics of a program to derive a unique fingerprint that is stored in a database (page 3, lines 8-13). Once the program is distributed and received elsewhere, another analysis is conducted on the received program in order to extract the fingerprint and compare it to the stored fingerprints in search of a match (Id.). The disclosed embodiments combine the use of watermarking and fingerprinting techniques in a way that enables a highly accurate, expedient and comprehensive reporting of program usage that also thwarts manipulation attempts by those who seek to divert royalty payments by fraudulently representing an interest in a work (page 4, lines 2-6 and page 17, lines 7-10).

Claim 2 of the present application relates a method of tracking a broadcast program that comprises inserting a unique watermark value into a program to be broadcast. This feature of claim 2 is described at, for example, page 7, lines 11-16, and page 9, lines 6-8, of the originally filed specification and depicted in step [002] in Figure 1 of the present application. The method of claim 2 further comprises deriving a fingerprint value based on the program's content (step [002] in Figure 1 and page 9, lines 16-20). In one example, the fingerprinting process can include analyzing a series of video frames to derive specific parameters, such as gamma, chroma and luminance, for the video frames (dashed box in Figure 2 and page 10, lines 5-21). Claim 2 also recites storing the program's watermark value and associated fingerprint value (page 12, lines 15-16 and page 13, lines 5-7).

The method of claim 2 further includes detecting any watermark value inserted in a given broadcast program (step [302g] in Figure 4 and page 13, lines 14-15). The originally filed specification describes that the detection of watermarks may be carried out by computers that are located at monitoring stations that receive a variety of broadcast channels through VHF, UHF, Satellite and Internet connections (dashed box in Figure 2 and page 13, lines 10-14). Claim 2 further recites deriving a fingerprint value based on the given broadcast program's content (steps [302a] to [302f] in Figure 4 and page 13, lines 15-17). As described in the originally filed specification, the derivation of fingerprints may involve analyzing the program’s content to produce several parameters (Id.).

The next feature of claim 2 relates to creating a database in which the unique watermark(s) and their associated derived fingerprint values for a plurality of unique programs to be broadcast are stored (page 4, line 16; page 12, lines 15-16; page 12, line 19 to page 13, line 7). The method of claim 2 further includes registering the unique watermark and associated derived fingerprint value for the program to be broadcast in the database (Figure 3 and page 11, line 14 to page 13, line 7). The originally filed specification describes that the registration can include operations such as verifying whether or not the watermark is correct and unique (step [206] in Figure 3), verifying whether or not the associated fingerprint is unique (step [210] in Figure 3) and sending reports to the applicant (step [222] in Figure 3).

The next operation that is recited in claim 2 includes redundantly identifying the given broadcast program using both a watermark and a fingerprint to verify the content. In particular, first, claim 2 recites that such redundant identification comprises comparing any detected watermark value with said database of registered watermark values. Step [306] in Figure 4 and page 14, lines 6-7, of the originally filed specification, describe that once the watermarks are detected, they are checked against the database of registered watermarks. Claim 2 further recites that if a detected watermark value matches a registered watermark value from the database of registered watermark values, cross-checking the fingerprint value derived from the given broadcast program against the database of registered fingerprints. This aspect of claim 2 is illustrated, for example, in steps [308] and [310] of Figure 4, as well as the corresponding description at page 15, lines 3-4, of the originally filed specification.

The next feature of claim 2 recites that if the fingerprint matches a registered fingerprint from the database of registered fingerprints, a first identification information associated with the registered watermark value is compared with a second identification information associated with the registered fingerprint to assess a status of the broadcast program. For example, if the detected watermarks match a Registration (which can include title, owner, unique watermark identification value, and other information – see, e.g., page 11, lines 1-6), the fingerprint is also matched against the database to determine whether or not both the fingerprint and watermark are registered to the same program (page 15, lines 3-6).

Claim 10 of the present application relates to a method for enabling reliable identification of a content. Claim 10 recites features similar to those recited in claim 2 but are formulated from the point of view of an entity that performs watermark embedding, fingerprint generation and registration of the content. Specifically, claim 10 recites embedding a watermark value into the content to produce an embedded content (page 7, lines 11-16; page 9, lines 6-8; and step [002] in Figure 1) and generating a fingerprint associated with the content (step [002] in Figure 1 and page 9, lines 16-20). Claim 10 further recites registering information comprising the watermark value and the fingerprint, where combination of the registered watermark value and fingerprint are subsequently used to redundantly identify the content (Figure 3 and page 11, line 14 to page 13, line 7). For example, the originally filed specification describes that the registration can include operations such as verifying whether or not the watermark is correct and unique (step [206] in Figure 3), verifying whether or not the associated fingerprint is unique (step [210] in Figure 3) and sending reports to the applicant (step [222] in Figure 3).

Claim 10 additionally recites that the redundant identification comprises generating a fingerprint associated with a received content (steps [302a] to [302f] in Figure 4 and page 13, lines 15-17) and analyzing the received content to detect at least one watermark value (step [302g] in Figure 4 and page 13, lines 14-15). The redundant monitoring of claim 10 also comprises identifying the received content by comparing the detected watermark value with a database of registered watermark values (step [306] in Figure 4 and page 14, lines 6-7). According to claim 10, if the detected watermark value matches a registered watermark value from the database of registered watermark values, the fingerprint is compared with a database of registered fingerprints (steps [308] and [310] of Figure 4; page 15, lines 3-4). Claim 10 also recites that if the derived fingerprint matches a registered fingerprint from the database of registered fingerprints, a first identification information associated with the stored watermark value is compared with a second identification information associated with the fingerprint to assess a status of the received content. For example, if the detected watermarks match a Registration (which can include title, owner, unique watermark identification value, and other information – see, e.g., page 11, lines 1-6), the fingerprint is also matched against the database to determine whether or not both the fingerprint and watermark are registered to the same program (page 15, lines 3-6).

Claim 32 of the present application relates to a method for enabling reliable identification of a received content. The features of claim 32 are similar to those recited in claim 2 but are formulated from the point of view of an entity that receives the broadcast content. Specifically, claim 32 recites generating a fingerprint associated with the received content (step [002] in Figure 1 and page 9, lines 16-20) and analyzing the received content to discern the presence of embedded watermarks (step [302g] in Figure 4 and page 13, lines 14-15). Claim 32 further recites identifying the received content in accordance with a plurality of registered fingerprint and watermark values and by redundant utilization of both of the generated fingerprint and the analyzing (step [306] in Figure 4; page 14, lines 6-7; steps [308] and [310] of Figure 4; page 15, lines 3-4).

The next feature of claim 32 recites that at least one watermark value is detected as a result of the analyzing (step [302g] in Figure 4 and page 13, lines 14-15). According to claim 32, identifying the received content comprises comparing a detected watermark value with a database of registered watermark values (step [306] in Figure 4 and page 14, lines 6-7). Claim 32 further recites that if the detected watermark value matches a registered watermark value from the database of registered watermark values, the fingerprint is compared with a database of registered fingerprints (steps [308] and [310] of Figure 4; page 15, lines 3-4). In addition, claim 32 recites that if the fingerprint matches a registered fingerprint from the database of registered fingerprints, a first identification information associated with the stored watermark value is compared with a second identification information associated with the fingerprint to assess a status of the received content. For example, if the detected watermarks match a Registration (which can include title, owner, unique watermark identification value, and other information – see, e.g., page 11, lines 1-6), the fingerprint is also matched against the database to determine whether or not both the fingerprint and watermark are registered to the same program (page 15, lines 3-6).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to be reviewed in this appeal are:

1) the rejection of claims 2, 4, 6, 7, 10-14, 17-19, 24-27, 32, 33, 36, 38, 40 and 42 under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent No. 7,020,304 to Alattar *et al.* (hereinafter "Alattar") in view of U.S. Patent No. 7,289,643 to Brunk *et al.* (hereinafter "Brunk"); and

2) the rejection of claims 3, 15, 16, 20-23, 28-31, 35 and 39 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Alattar and Brunk, in view of one or more of the following references: U.S. Patent No. 6,912,010 to Baker *et al.* (hereinafter "Baker"), U.S. Patent Publication No. 2002/0054089 to Nicholas *et al.* (hereinafter "Nicholas"), U.S. Patent No. 6,785,815 to Serret-Avila *et al.* (hereinafter "Serret-Avila"), U.S. Patent No. 6,915,422 to Nakamura (hereinafter "Nakamura") and U.S. Patent No. 6,487,301 to Zhoa (hereinafter "Zhoa").

ARGUMENT

I. Rejection of Claims 2, 4, 6, 7, 10-14, 17-19, 24-27, 32, 33, 36, 38, 40 and 42

Claims 2, 4, 6, 7, 10-14, 17-19, 24-27, 32, 33, 36, 38, 40 and 42 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Alattar in view of Brunk. In particular, in rejecting claim 2 of the present application, the Examiner has relied upon Alattar to assert that this reference describes all the features of pending claim 2, except for redundant identification of the content (Office Action, dated September 2, 2009, page 4, line 1 to page 5, line 12). The Examiner has then argued that Brunk describes the various features that are associated with redundant identification of the content, as is recited in pending claim 2 (Office Action, dated September 2, 2009, page 5, line 19 to page 7, line 9). The Examiner has made similar arguments against pending independent claims 10 and 32 (Office Action, dated September 2, 2009, pages 9-11 and 14-17).

A. Requirements for a *prima facie* case of obviousness

In *In re Rijckaert*, 9 F.3d 1531, 1532, (Fed. Cir. 1993), the Federal Circuit outlined the burden on the PTO as follows:

> In rejecting claims under 35 U.S.C. 103, the examiner bears the initial burden of presenting a *prima facie* case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. *Id*. "A *prima facie* case of obviousness is established when the teachings from the prior art itself would appear to have suggested the claimed subject matter to a person of ordinary skill in the art. " *In re Bell*, 991 F.2d 781, 782, 26 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1993) (quoting *In re Rinehart*, 531 F.2d 1048, 1051, 189 U.S.P.Q. 143, 147 (CCPA 1976)). If the examiner fails to establish a *prima facie* case, the rejection

> is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1988).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some reasonable suggestion or motivation to modify the prior art reference or to combine reference teachings. Second, there must be a reasonable expectation of success of achieving the desired goals. Finally, the prior art references when combined must teach all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the Appellant's disclosure. *In re Vaeck*, 947 F.2d 488 (Fed. Cir. 1991). In the present case, these criteria are not met.

B. Alattar and/or Brunk fail to teach or suggest "*comparing any detected watermark value with said database of registered watermark values, and if a detected watermark value matches a registered watermark value from said database … , cross-checking said fingerprint value derived from said given broadcast program against said database of registered fingerprints*"

Pending claims 2, 10 and 32 specifically recite that redundantly identifying the broadcast program comprises three separate operations:

> (1) comparing any detected watermark value with the database of registered watermark values;
>
> (2) if a detected watermark value matches a registered watermark value from said database of registered watermark values, cross-checking said fingerprint value derived from said given broadcast program against said database of registered fingerprints; and
>
> (3) if said derived fingerprint matches a registered fingerprint from said database of registered fingerprints, a first identification information associated with said registered watermark value is compared with a second identification information associated with said registered fingerprint.

The pending claims are, at a minimum, distinguishable from the disclosure of Alattar and Brunk in that these cited references fail to describe the operations identified by (1) and (2) above.

B-1. Alattar fails to teach or suggest using watermarks and fingerprints for redundant identification

In rejecting operation (1) of the pending claims, the Examiner is relying on Alattar col. 10, lines 10-18, to argue that this section of Alattar describes a database that contains information related to watermarks, including additional identification information (Office Action, dated September 2, 2009, page 5, lines 4-8). In rejecting operation (2) of the pending claims, the Examiner is arguing that Alattar, in col. 20, lines 38-57, also describes checking the fingerprint value against a database of fingerprints (Office Action, dated September 2, 2009, page 5, lines 9-12). Appellant respectfully disagrees.

Alattar's disclosure regarding the use of a watermark and a fingerprint is entirely different from the features recited in pending claims 2, 10 and 32. In particular, one portion of Alattar relied upon by the Examiner (i.e., Alattar, col. 10, lines 10-36) describes comparing the extracted watermark values alone to a stored database of values, without any discussions related to fingerprints or content signatures. Further, another portion of Alattar relied upon by the Examiner (i.e., Alattar, col. 20, lines 20-57) describes the use of both watermarks and fingerprints. However, this portion of Alattar discloses, when a watermark and a fingerprint are used together, the watermark serves as a calibration signal in order to align the content before computing the fingerprint. However, there are no teachings or suggestions in Alattar related to using the watermark and fingerprints for redundant identification of a program, as is recited in the pending claims.

In response to Appellant's arguments, the Examiner acknowledges that Alattar does not clearly teach redundant identification of the content as recited in the pending claims (Examiner's Answer page 27, lines 13-16). However, the Examiner alleges that Brunk, when used in combination with Alattar, renders the above-noted features of the pending claims obvious (Examiner's Answer page 28, lines 3-14).

As will be discussed in the sections that follow, Appellant respectfully disagrees with the Examiner's position since Brunk fails to cure the deficiencies of Alattar. Moreover, Appellant respectfully submits that the Examiner is relying on impermissible hindsight in alleging that a person of ordinary skill in the art would have been able to combine the teachings of Alattar and Brunk, and to further contemplate additional features of the pending claims that are not taught or suggested in either Alattar or Brunk.

B-2. Brunk fails to teach or suggest using watermarks and fingerprints for redundant identification

The Examiner has also relied in-part on Brunk, col. 6, line 65 to col. 7, line 50; col. 8, line 64 to col. 9, line 1; and several other sections of Brunk, to assert that Brunk describes redundant identification of the content in the context of the pending claims (Office Action, dated September 2, 2009, page 6, lines 6-13). Appellant respectfully disagrees.

The above-noted sections of Brunk fail to teach or suggest the use of both the watermark and the fingerprint for redundant identification of a content. To the contrary, these sections of Brunk describe using the watermarks to carry information additional to (and different from) what is conveyed by the content signatures (Brunk, col. 6, line 65 to col. 7, line 3). In the example scenario described in Brunk's disclosure, a watermark is used to identify the owner of a music content, whereas the content signature (i.e., purportedly the fingerprint) is used to determine the name and version of the song (Brunk, col. 7, lines 4-29). As such, these sections of Brunk fail to teach or suggest the use of both fingerprints and watermarks to enable redundant identification of a program.

B-3. Alattar and/or Brunk fail to teach or suggest utilizing watermarks and fingerprints in the manner recited in the pending claims

The Examiner is also arguing that since Alattar and Brunk describe using content signatures and watermarks to carry certain information, it would have been obvious to a person of ordinary skill in the art to realize that the two may carry the same or very similar information to redundantly identify a content (Examiner's Answer, page 29, lines 12-16; Office Action dated September 2, 2009, page 2, lines 7-23). The Examiner is further arguing that Brunk, in col. 6, lines 40-52, describes redundant monitoring since it describes that "a content signature can also be compared to digital watermark data and if the content signature and digital watermark data match (or otherwise coincide) the content is determined to be authentic" (Examiner's Answer, page 29, lines 19-22; Office Action dated September 2, 2009, page 3, lines 6-7; page 6, line 8). Appellant respectfully disagrees.

According to MPEP § 2141.01:

> It is difficult but necessary that the decisionmaker forget what he or she has been taught . . . about the claimed invention and cast the mind back to the time the invention was made … to occupy the mind of one skilled in the art.

Appellant respectfully submits that the Examiner assertions regarding the obviousness of the pending claims are conclusory statements that are reached through impermissible hindsight.

Further, the obviousness rejections that are asserted by the Examiner are based on an irrelevant misconstruction of the claims. In support of the obviousness rejections based in-part on Brunk's disclosure, the Examiner implies that the "redundant" identification, as claimed, means simply that the watermark and the fingerprint carry the same information. In particular, in the Examiner's Answer at page 28, lines 9-11, the Examiner states:

> A person of ordinary skill in the art would have known the similarities in the content signature data and the watermark data and realized that the two may carry the same or very similar data… to identify the content. Therefore, the content signature and watermark data may be used to "redundantly" identify the content.

Similar statements are made in the Examiner's Answer at page 29, lines 12-16, and at page 31 lines 7-11. This is not a valid basis for the obviousness rejections because the claims do not even require that the watermark carry the same information as the fingerprint. In fact, the watermark and fingerprint are unlikely to carry the same information, since the watermark carries a predetermined set of embedded data, while the fingerprint is derived from the content itself. Hence, the Examiner has not established a *prima facie* case of obviousness.

Nevertheless, even if, as alleged by the Examiner, the watermarks and content signatures that are described in Alatter and Brunk convey the same or similar information, there are no teachings or suggestions in these references to indicate the use of these watermarks and fingerprints in a manner that is recited in the pending claims. In particular, these references fail to teach or suggest detecting the watermarks, comparing the detected values to a database, if a match is found, cross-checking a derived fingerprint against a database of registered fingerprints.

Further, the above-noted section of Brunk (i.e., col. 6, lines 40-52) merely describes comparing data conveyed directly within a watermark to a content signature itself. In particular, this section of Brunk teaches that the watermark itself contains a content signature. Such a comparison, however, contrary to the Examiner's assertions, does not teach or suggest operations (1) and (2) of the pending claims. In particular, operations (1) and (2) recite matching the detected watermark values and the derived fingerprints against databases of registered fingerprints and watermarks, respectively. Such operations enable identification of the content even in scenarios where watermarks are not detected with proper values and/or if the detected watermarks fail to match the derived fingerprints. For example, due to noise or interference in the broadcast channel, as well as intentional or fraudulent tampering with the content, the received broadcast content can contain errors or imperfections that produce incorrectly detected watermarks. Such erroneous detections can occur if a watermark payload is "mis-decoded" as another watermark payload, or when "false" watermarks are detected from a received content with no embedded watermarks (i.e., false positive detections). The watermarks that are produced due to mis-decodes and/or false positive detections, however, may still result in a match when compared to the database of stored watermarks. In such scenarios, operation (2) that is recited in pending claim 2 provides a second level of identification and/or affirmation capability that enables the identification of the content even if a watermark is mis-decoded or is falsely detected.

In contrast, in the above-described scenarios where a watermark is erroneously detected, the "comparing" of the watermark payload to the content signature as described in Brunk's disclosure (i.e., col. 6, lines 40-52) may indicate that the content has been modified (because the content signature data incorrectly detected from the watermark is very unlikely to match the content signature derived from the received content), but the content will not be identified. As such, the mere comparison of a content signature to a watermark value, which is described in Brunk's disclosure fails to provide the full identification capabilities that are obtained through operations (1) and (2) of the pending claims. Therefore, operations (1) and (2) of the pending claims are not taught or suggested by Brunk's disclosure.

Further, as noted earlier, Alattar fails to teach or suggest the features of the pending claims that are recited in operations (1) and (2).

C. Alattar and/or Brunk fail to teach or suggest "*if said derived fingerprint matches a registered fingerprint from said database of registered fingerprints, a first identification information associated with said registered watermark value is compared with a second identification information associated with said registered fingerprint*"

Pending claims 2, 10 and 32 specifically recite that redundant identification of the broadcast program also comprises:

> (3) if said derived fingerprint matches a registered fingerprint from said database of registered fingerprints, a first identification information associated with said registered watermark value is compared with a second identification information associated with said registered fingerprint.

The pending claims are, at a minimum, distinguishable from the disclosure of Alattar and Brunk in that these cited references fail to describe the operations identified by (3) above.

C-1. Alattar and/or Brunk fail to teach or suggest "*a first identification information associated with said registered watermark value is compared with a second identification information associated with said registered fingerprint*"

In accordance with the pending claims, once a watermark has been detected and matched against a database of registered watermarks and a fingerprint has been derived and matched against a database of registered fingerprints, a first identification information associated with said registered watermark value is compared with a second identification information associated with said registered fingerprint. As such, the process of redundant identification, according to the pending claims, additionally comprises comparing certain identification information associated with the watermarks with certain other identification information associated with the registered fingerprints. The claimed comparing of identification information associated with the watermark with identification information associated with the fingerprint is not taught or suggested by Brunk, Alattar or any other references of record.

In alleging disclosure of this feature in the prior art, the Examiner is relying on Brunk's direct "comparing" of a content signature and a watermark value (i.e., Brunk, col. 6, lines 40-52) by further reasoning that "the fingerprint and the watermark may both contain the same information and when compared the information will coincide to prove the content to be authentic or will be different and prove the content to be modified in some way" (Office Action dated September 2, 2009, page 7, lines 1-9). Appellant respectfully disagrees.

First, the Examiner is overlooking the fact that the above-noted feature of the pending claims, identified as operation (3), is different from, and is performed in addition to, the features related to operations (1) and (2). However, the Examiner is using the same sentence from Brunk's disclosure (i.e., Brunk, col. 6, lines 40-52) to argue that Brunk describes redundant identification of a content according to operations (1) and (2), as well as operation (3). Such an assertion is not supported by Brunk's disclosure and/or an understanding of a person of ordinary skill in the art, as the teaching in Brunk of a mere comparison of a watermark value to a content signature does not, in any way, teach or suggest all the various features that are recited in operations (1), (2) and (3) of the pending claims.

Second, the comparison of a content signature to a watermark value is an entirely different operation than what is recited in operation (3). It appears that the Examiner is misconstruing operation (3) of the pending claims by characterizing this operation as comparing a "watermark value" to a "fingerprint value" (Examiner's Answer, page 29, lines 16-18). Such a construction is not consistent with what is being recited in pending claim 2 as part of the above noted operation (3). As discussed earlier, operation (3) states comparing a first identification information <u>associated with said registered watermark value</u> with a <u>second identification information associated with said registered fingerprint</u>. Moreover, the pending claims specifically recite a "[derived] fingerprint," a "registered fingerprint," a "registered watermark value," a "first identification information" and a "second identification information." The above-noted section of Brunk's description (i.e., Brunk, col. 6, lines 40-52) merely describes the comparison of two values (i.e., a watermark value and a content signature), which cannot be construed as teaching or suggesting the interactions between the at least five values that are recited in the pending claims.

Because of operation (3), the claimed invention provides an additional assurance that content is authentic and not tampered with. For example, it is possible for content to have a valid registered watermark, passing operation (1), and to have a valid registered fingerprint, passing operation (2), but still be rejected under operation (3) because the identification information associated with the watermark and the identification information associated with the fingerprint reveal that the two are (or are not) registered to the same program.

Further, as noted earlier, Alattar fails to teach or suggest the above noted features of the pending claims that relate to redundant identification of a program.

C-2. The methodologies of Alattar and/or Brunk fail to provide many capabilities associated with redundant identification that is recited in the pending claims

Unlike the redundant monitoring that is effected according to the pending claims, Alattar and/or Brunk's comparison of the content signature and a watermark value fails to properly operate and/or identify the proper content if in each of the following example scenarios:

A) watermarks are mis-decoded or falsely detected (e.g., a wrong content owner is identified),

B) derived fingerprints are mis-decoded or falsely detected (e.g., an incorrect version of the song is identified), and/or

C) both the detected watermarks and derived fingerprints are mis-decoded or falsely detected.

As noted earlier, scenarios (A) through (C) can occur due to intentional, and perhaps fraudulent, tampering with the program content. In addition, the above scenarios can occur due to errors that are introduced into the program content during its broadcast through a noisy transmission channel (e.g., terrestrial broadcast, Internet transmission, etc.). In such cases, the watermarks and fingerprints that are obtained from the received content may have incorrect values (i.e., due to mis-decodes or false detections).

In scenario (A), Alattar's and/or Brunk's schemes fail to properly identify the content. In particular, if the watermark payload is simply compared to the derived fingerprint, no identification of the content is produced by Alattar/Brunk methodologies. In the scheme where the watermark and fingerprint identify the content owner and the song version, respectively, the wrong content owner is identified when a false watermark value is detected. Similarly, in scenario B, the comparison of the watermark payload and the content signature that is described in Brunk produces no match whatsoever. The use of Brunk's other scheme, in which the watermark and fingerprint identify the content owner and the song version, respectively, results in the identification of the wrong song version. Finally, in scenario (C), the above noted schemes of Brunk/Alattar result in either no identification or in erroneous identification of both the content owner and the song version. Therefore, the disclosure of Brunk and/or Alattar fail to produce proper identification in at least scenarios (A) through (C). Furthermore, there are no teachings or even suggestions in Brunk or Alattar to indicate that such scenarios are contemplated or that they can be addressed through redundant identification of the content, as is recited in the pending claims.

In contrast, through the above-described operations (1), (2) and (3) of the pending claims, a false identification of a received content can still be avoided, even when faced with these scenarios. In particular, as illustrated in the flow diagram of Figure 4, and described at pages 13-17 of the originally filed specification, the different levels of cross-checking of the derived fingerprint, the registered fingerprint, the registered watermark value, the first identification information and the second identification information allows the proper identification of the content. For example, in scenarios (A) and (B), operations (1) and (2) of the pending claims can prevent a content from being falsely identified, whereas in scenario

(C), operation (3) provides an additional level of assurance that prevents false identification of the content.

D. The references of record fail to render the features of pending claims 2, 4, 6, 7, 10-14, 17-19, 24-27, 32, 33, 36, 38, 40 and 42 obvious

As discussed in sections (B) and (C), Alattar and/or Brunk fail to teach or suggest all of the features of pending independent claims 2, 10 and 32.

Therefore, a *prima facie* case of obviousness has not been established. Accordingly, claims 2, 10 and 32 are patentable.

As to claims 4, 6, 7, 11-14, 17-19, 24-27, 33, 36, 38, 40 and 42, these claims depend, either directly or indirectly, from one of allowable claims 2, 10 or 32 and are, therefore, patentable for at least that reason, as well as for additional patentable features when these claims are considered as whole.

II. Rejection of Claims 3, 15, 16, 20-23, 28-31, 35 and 39

Claims 3, 15, 16, 20-23, 28-31, 35 and 39 under 35 U.S.C. § 103(a) stand rejected as allegedly being unpatentable over Alattar and Brunk, in view of one or more of the following references: Baker, Nicholas Serret-Avila, Nakamura and Zhoa.

The Examiner has relied upon references Baker, Nicholas Serret-Avila, Nakamura and Zhoa to argue against the specific features that are recited in dependent claims 3, 15-16, 20-23, 28-31, 35 and 39. However, none of these references cure the above-noted deficiencies of Alattar and/or Brunk that were discussed in connection with pending claims 2, 10 and 32. Claims 3, 15, 16, 20-23, 28-31, 35 and 39 depend, either directly or indirectly, from one of allowable claim 2, 10 or 32 and are, therefore, patentable for at least that reason, as well as for additional patentable features when these claims are considered as a whole.

III. Conclusion

The pending claims of the present application recite patentable subject matter and are in condition for allowance. The rejections made by the Examiner should be withdrawn.

CLAIMS APPENDIX

1.(Canceled).

2. (Currently Rejected) A method of tracking a broadcast program, comprising:

inserting a unique watermark value into a program to be broadcast;

deriving a fingerprint value based on said program's content;

storing said program's watermark value and associated fingerprint value;

detecting any watermark value inserted in a given broadcast program;

deriving a fingerprint value based on said given broadcast program's content;

creating a database in which said unique watermark(s) and their associated derived fingerprint values for a plurality of unique programs to be broadcast are stored;

registering said unique watermark and associated derived fingerprint value for said program to be broadcast in said database; and

redundantly identifying said given broadcast program, said redundant identification comprising:

comparing any detected watermark value with said database of registered watermark values;

if a detected watermark value matches a registered watermark value from said database of registered watermark values, cross-checking said fingerprint value derived from said given broadcast program against said database of registered fingerprints; and

if said fingerprint matches a registered fingerprint from said database of registered fingerprints, a first identification information associated with said registered watermark value is compared with a second identification information associated with said registered fingerprint to assess a status of said broadcast program.

3. (Currently Rejected) The method of claim 2, wherein said unique watermark value is written into the user bits of said program's SMPTE time code.

4. (Currently Rejected) The method of claim 2, wherein:

said program to be broadcast has an associated embedded audio data stream; and

said unique watermark is encoded into the bits of said program's embedded audio data stream.

5. (Canceled).

6. (Currently Rejected) The method of claim 2, further comprising reporting the results of said cross-checking to a registrant of said program to be broadcast.

7. (Currently Rejected) The method of claim 2, further comprising comparing said fingerprint value derived from said given broadcast program with said stored fingerprint values when said fingerprint value derived from said given broadcast program is different than said stored fingerprint value associated with said stored watermark.

8. (Canceled).

9. (Canceled).

10. (Currently Rejected) A method for enabling reliable identification of a content comprising:

embedding a watermark value into said content to produce an embedded content;

generating a fingerprint associated with said content;

registering information comprising said watermark value and said fingerprint, wherein combination of said registered watermark value and fingerprint are subsequently used to redundantly identify said content, said redundant identification comprising:

generating a fingerprint associated with a received content;

analyzing said received content to detect at least one watermark value;

identifying said received content by comparing said detected watermark value with a database of registered watermark values;

if said detected watermark value matches a registered watermark value from said database of registered watermark values, said fingerprint is compared with a database of registered fingerprints; and

if said derived fingerprint matches a registered fingerprint from said database of registered fingerprints, a first identification information associated with said stored watermark value is compared with a second identification information associated with said fingerprint to assess a status of said received content.

11. (Currently Rejected) The method of claim 10, wherein said fingerprint is generated by analyzing inherent characteristics of the content.

12. (Currently Rejected) The method of claim 10, wherein said inherent characteristics comprise at least one of luminance, chroma, gamma, or amplitude levels of the content.

13. (Currently Rejected) The method of claim 10, wherein said fingerprint is generated for at least portions of an audio or video component of said signal.

14. (Currently Rejected) The method of claim 10, wherein said watermark value is embedded in at least portions of an audio or video component of said content.

15. (Currently Rejected) The method of claim 10, wherein said watermark value is inserted into an auxiliary information area of said content.

16. (Currently Rejected) The method of claim 15, wherein said auxiliary information area is reserved for an SMPTE time code.

17. (Currently Rejected) The method of claim 10, wherein said registering comprises:

receiving information comprising at least said watermark value and said fingerprint at a registration authority; and

verifying the received information.

18. (Currently Rejected) The method of claim 17, wherein said verifying comprises comparing at least one of said watermark value or said fingerprint against a database of registered watermark values and fingerprints.

19. (Currently Rejected) The method of claim 18, wherein said registering is completed when said comparing produces no matches.

20. (Currently Rejected) The method of claim 18, wherein production of at least one match as a result of said comparing is indicative of an incomplete registration.

21. (Currently Rejected) The method of claim 20, further comprising notifying at least one of an applicant or a content owner.

22. (Currently Rejected) The method of claim 18, wherein, said registering is partially completed when said comparing produces at least one match.

23. (Currently Rejected) The method of claim 22, further comprising:
contacting at least one of an applicant for registration or a content owner; and
updating said database in accordance with the response(s) of said applicant or said content owner.

24. (Currently Rejected) The method of claim 17, further comprising receiving additional content identification information.

25. (Currently Rejected) The method of claim 24, wherein said additional content identification information comprises at least one of content title, ownership information, or origination information.

26. (Currently Rejected) The method of claim 24, further comprising:

comparing at least one of said watermark value, said fingerprint or said additional content information against a database of registered watermark values, fingerprints and additional content identification information.

27. (Currently Rejected) The method of claim 26, wherein said registering is completed when said comparing produces no matches.

28. (Currently Rejected) The method of claim 26, wherein said registering is not completed when said comparing produces at least one match.

29. (Currently Rejected) The method of claim 28, further comprising notifying at least one of an applicant for registration or a content owner.

30. (Currently Rejected) The method of claim 26, wherein said registering is partially completed when said comparing produces at least one match.

31. (Currently Rejected) The method of claim 30, further comprising:

contacting at least one of an applicant for registration or a content owner; and

updating said database in accordance with the response(s) of said applicant or said content owner.

32. (Currently Rejected) A method for enabling identification of a received content comprising:

generating a fingerprint associated with said received content;

analyzing said received content to discern the presence of embedded watermarks; and

identifying said received content in accordance with a plurality of registered fingerprint and watermark values and by redundant utilization of both of said generated fingerprint and said analyzing, wherein:

at least one watermark value is detected as a result of said analyzing;

said identifying comprises comparing a detected watermark value with a database of registered watermark values;

if said detected watermark value matches a registered watermark value from said database of registered watermark values, said fingerprint is compared with a database of registered fingerprints; and

if said fingerprint matches a registered fingerprint from said database of registered fingerprints, a first identification information associated with said stored watermark value is compared with a second identification information associated with said fingerprint to assess a status of said received content.

33. (Currently Rejected) The method of claim 32, wherein said identifying is based on additional information stored in a registration database.

34. (Canceled).

35. (Currently Rejected) The method of claim 32, wherein:

no watermarks are detected as a result of said analyzing;

said identifying comprises comparing said fingerprint with a database of registered fingerprints; and

if no matches are discovered, reporting the reception of an unregistered content.

36. (Currently Rejected) The method of claim 32, wherein:

at least one watermark value is detected as a result of said analyzing; and

the detected watermark value and said fingerprint are combined to uniquely identify said received content.

37. (Canceled).

38. (Currently Rejected) The method of claim 32, wherein an agreement between said first and second identification information indicates the reception of a properly registered content.

39. (Currently Rejected) The method of claim 32, wherein a report is issued in the event of a conflict between said first and second identification information.

40. (Currently Rejected) The method of claim 32, wherein a conflict between said first and second identification information indicates the reception of an improperly registered content or an altered content.

41. (Canceled).

42. (Currently Rejected) The method of claim 32, wherein cryptographic techniques are employed to ensure secure communications with said database.

EVIDENCE APPENDIX

No evidence is relied upon in this brief.

RELATED PROCEEDINGS APPENDIX

There are no orders or opinions in any related cases.

Respectfully submitted,

Date October 27, 2010

By /Babak Tehranchi/

FOLEY & LARDNER LLP
Customer Number: 30542
Telephone: (858) 847-6727
Facsimile: (858) 792-6773

Babak Tehranchi
Attorney for Appellant
Registration No. 55,937